

# SQUARE-FREE VALUES OF REDUCIBLE POLYNOMIALS

ANDREW R. BOOKER AND T.D. BROWNING

**ABSTRACT.** We calculate admissible values of  $r$  such that a square-free polynomial with integer coefficients, no fixed prime divisor and irreducible factors of degree at most 3 takes infinitely many values that are a product of at most  $r$  distinct primes.

## 1. INTRODUCTION

Let  $H \in \mathbb{Z}[x]$  be a non-constant square-free polynomial of degree  $h$  with  $\kappa$  irreducible factors. Unless there is good reason to suppose otherwise, one expects that  $H(n)$  is square-free infinitely often. In fact, assuming that  $H$  has no *fixed prime divisor*, one expects that  $H(n)$  is a product of precisely  $\kappa$  distinct primes for infinitely many values of  $n \in \mathbb{Z}$ . We shall assume that  $H$  has no fixed prime divisor in all that follows, by which we mean that there is no prime  $p$  such that  $p \mid H(n)$  for every  $n \in \mathbb{Z}$ .

When  $\kappa = 1$  and  $h = 3$  it follows from work of Erdős [11] that  $H(n)$  is square-free infinitely often. This fact has not yet been extended to a single irreducible quartic polynomial, although work of Granville [13] handles irreducible polynomials of arbitrary degree under the *abc conjecture*. On the other hand, thanks to work of Hooley [15], in the setting of irreducible cubic polynomials we have an asymptotic formula for the number of  $n \leq x$  for which  $H(n)$  is square-free. Recent work of Reuss [19] has substantially improved this asymptotic formula, with the outcome that we now have a power saving in the error term.

The topic of almost-prime values of polynomials has been studied extensively by several authors. The *DHR weighted sieve* of Diamond, Halberstam and Richert (see [5, 6]) gives an efficient means of producing values of  $r$  such that  $\Omega(H(n)) \leq r$  for infinitely many  $n \in \mathbb{Z}$ , where  $\Omega(m)$  is the total number of prime factors of  $m$  counted with multiplicity. The following result gives sufficient conditions on polynomials  $H$ , not necessarily irreducible, under which  $H(n)$  takes infinitely many values that are simultaneously square-free and have at most  $r$  prime factors, for relatively small values of  $r$ .

**Theorem 1.1.** *Assume that  $H$  has no fixed prime divisor and that each irreducible factor of  $H$  has degree at most 3. Then there exists  $r \in \mathbb{N}$  such that*

$$\sum_{\substack{n \leq x \\ \Omega(H(n)) \leq r}} \mu^2(H(n)) \gg \frac{x}{(\log x)^\kappa}.$$

*Admissible values of  $r$  are recorded in Table 1 for  $h \leq 20$  and at [3] for  $h \leq 50$ .*

One of our motivations for this work is the following application derived in [2]. Given any finite set of prime numbers, Euclid showed how to obtain another prime not in the set. Applied iteratively beginning with a single prime, one obtains an infinite sequence of distinct

---

*Date:* June 1, 2016.

*2010 Mathematics Subject Classification.* 11N36 (11N32).

$h \setminus \kappa$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	1																			
2	2	5																		
3	4	6	8																	
4		7	10	12																
5		8	11	13	16															
6		9	12	15	18	20														
7			13	16	19	22	25													
8			14	17	20	23	26	29												
9			16	19	22	25	28	31	34											
10				20	23	26	29	33	36	39										
11				21	24	27	31	34	37	41	44									
12				22	25	29	32	35	39	42	45	49								
13					27	30	33	37	40	44	47	51	54							
14					28	31	35	38	42	45	49	52	56	59						
15					29	33	36	40	43	47	50	54	57	61	64					
16						34	37	41	45	48	52	55	59	62	66	70				
17						35	39	42	46	50	53	57	60	64	68	71	75			
18						36	40	44	47	51	55	58	62	66	69	73	77	80		
19							41	45	49	52	56	60	63	67	71	75	78	82	86	
20							42	46	50	54	57	61	65	69	73	76	80	84	88	92

TABLE 1. Admissible values of  $r$  for  $h \leq 20$ .

prime numbers. The set of all possible sequences obtained from a given starting prime  $p$  has the natural structure of a directed graph, say  $G_p$ , which one can then ask questions about; e.g., is  $G_p$  a tree? Applying Theorem 1.1 to the polynomial

$$H = (x^2 + x + 1)(x^2 + 1)(x^3 + x^2 + 2x + 1),$$

it was shown in [2] that  $G_p$  is not a tree for a positive proportion of  $p$ , and in fact there are infinitely many coprime pairs  $(a_i, q_i) \in \mathbb{N}^2$ , with  $(q_i, q_j) = 1$  for  $i \neq j$ , such that  $G_p$  has a loop of height at most 13 for any  $p \equiv a_i \pmod{q_i}$ .

For any  $z \geq 1$  let  $P(z) = \prod_{p \leq z} p$  and let  $\delta > 0$  be a small parameter to be chosen in due course. Our starting point in the proof of Theorem 1.1 is the observation that

$$\sum_{\substack{n \leq x \\ \Omega(H(n)) \leq r}} \mu^2(H(n)) \geq \sum_{\substack{n \leq x \\ \Omega(H(n)) \leq r \\ (H(n), P(x^\delta)) = 1}} \mu^2(H(n)) \geq \Sigma_1 - \Sigma_2,$$

where

$$\Sigma_1 = \# \{n \leq x : \Omega(H(n)) \leq r, (H(n), P(x^\delta)) = 1\}$$

and

$$\Sigma_2 = \# \{n \leq x : \exists p > x^\delta \text{ s.t. } p^2 \mid H(n)\}.$$

Our strategy is now evident. First we will seek a lower bound for  $\Sigma_1$ , for which we shall invoke the DHR weighted sieve [5] in §3. Next, in §4, we shall prove that there exists  $\eta > 0$  such that

$$\Sigma_2 = O(x^{1-\eta}), \tag{1.1}$$

provided that each irreducible factor of  $H$  has degree at most 3. The key input here will come from the work of Reuss [19] that we have already mentioned and which is based on the *approximate determinant method*. Finally, in §5, we shall turn to the question of optimising the value of  $r$  for which the lower bound in Theorem 1.1 holds.

A well-known feature of the weighted sieve is that any admissible value of  $r$  can only be derived through a precise analysis of certain integrals involving complicated functions  $\sigma, f, F$  that arise as solutions to certain differential-delay problems. These are all described in Theorem 3.1 below. Wheeler, in his thesis [21], gave algorithms for solving the differential-delay problem via Gaussian quadrature with rigorous error bounds, and some of the theoretical work concerning the solution of this problem (see [6] for a comprehensive treatment) relies on his computations. However, [21] is rather difficult to obtain and there appears to have been no published account of Wheeler's algorithms or source code. With this in mind, in §5 we describe an independent implementation based on polynomial approximations. Thanks to the exponential gains in computer power since Wheeler's thesis was written, we can afford to leave more of the work to the computer, to the point that our error estimates require nothing more complicated than the alternating series test or the Lagrange form of the remainder term in Taylor's theorem. We rely heavily throughout on Fredrik Johansson's excellent library `Arb` [17] for arbitrary-precision interval arithmetic. Thus, we make no assumptions about round-off error, so that, modulo bugs in the code or computer hardware, our results are rigorous. The end result of our computations is the online table [3] of minimum values of  $r$  for every pair  $\kappa, h$  with  $\kappa \leq h \leq 50$ , from which Table 1 is derived. The reader wishing to compute  $r$  for numbers outside of the tables is welcome to make use of our program, also available at [3].

We conclude the introduction by proving one more result used in [2]. Namely, if we drop the condition  $\Omega(H(n)) \leq r$  then we can promote the lower bound in Theorem 1.1 to an asymptotic formula by adapting work of Hooley [16, Chapter 4] and invoking Reuss' work. To do so we write

$$\sum_{n \leq x} \mu^2(H(n)) = N(x) + O(E(x) + \Sigma_2),$$

where  $\Sigma_2$  is as above and  $N(x)$  (resp.  $E(x)$ ) denotes the number of  $n \leq x$  for which  $H(n)$  is not divisible by  $p^2$  for any prime  $p \leq \frac{1}{6} \log x$  (resp. there exists a prime  $p \in (\frac{1}{6} \log x, x^\delta]$  such that  $p^2 \mid H(n)$ ). Combining the estimate [16, Eq. (125)] for  $N(x)$ , with (1.1) and the estimate [16, Eq. (127)] for  $E(x)$ , we arrive at the following result.

**Theorem 1.2.** *Assume that each irreducible factor of  $H$  has degree at most 3 and let*

$$\varrho(q) = \#\{\nu \bmod q : H(\nu) \equiv 0 \bmod q\}, \tag{1.2}$$

*for any  $q \in \mathbb{N}$ . Then*

$$\sum_{n \leq x} \mu^2(H(n)) = x \prod_p \left(1 - \frac{\varrho(p^2)}{p^2}\right) + O\left(\frac{x}{\log x}\right).$$

**Acknowledgements.** While working on this paper the first author was supported by *EP-SRC grant EP/L001454/1* and the second author was supported by *ERC grant 306457*.

## 2. POLYNOMIAL CONGRUENCES

An important function in our work is the multiplicative arithmetic function  $\varrho(q)$  that was defined in (1.2). Our assumption that  $H$  has no fixed prime divisor is equivalent to the statement that  $\varrho(p) < p$  for every prime  $p$ . We henceforth assume that

$$H(x) = H_1(x) \cdots H_\kappa(x)$$

for a system  $H_1, \dots, H_\kappa \in \mathbb{Z}[x]$  of pairwise non-proportional irreducible polynomials, with  $d_i = \deg(H_i)$  for  $1 \leq i \leq \kappa$ .

It will pay dividends to consider the general function

$$\varrho(G; q) = \#\{\nu \bmod q : G(\nu) \equiv 0 \bmod q\},$$

associated to any irreducible polynomial  $G \in \mathbb{Z}[x]$  of degree  $d$  and any  $q \in \mathbb{N}$ . Note that  $\varrho(G; q)$  is a multiplicative function of  $q$  and  $\varrho(q) = \varrho(H; q)$ . Assuming that  $p$  does not divide the content of  $G$ , we have the basic estimate

$$\varrho(G; p^k) \ll \begin{cases} 1, & \text{if } p \nmid \text{disc}(h), \\ p^{(1-1/d)k}, & \text{otherwise,} \end{cases} \quad (2.1)$$

where the implied constant is only allowed to depend on  $d$ . Here the first bound is a trivial application of Hensel's lemma, combined with the inequality  $\varrho(G; p) \leq d$ . The second estimate is well known (see [4, Lemma 2], for example).

Returning to  $\varrho(p^k)$  for a prime  $p$  and  $k \in \mathbb{N}$ , let

$$\Delta = 6 \prod_i |\text{disc}(H_i)| \prod_{i \neq j} |\text{Res}(H_i, H_j)|, \quad (2.2)$$

where  $\text{Res}(H_i, H_j)$  is the resultant of  $H_i$  and  $H_j$ . This is an integer which vanishes if and only if  $H_i$  and  $H_j$  share a common root. Our assumptions on the system  $H_1, \dots, H_\kappa$  imply that  $\Delta$  is a positive integer and we henceforth allow all of our implied constants to depend on it. Thus we clearly have  $\varrho(p^k) = O_k(1)$  if  $p \mid \Delta$ , where the implied constant depends on  $k$ . If  $p \nmid \Delta$ , then  $p$  doesn't divide any of the resultants  $\text{Res}(H_i, H_j)$ , and so

$$\varrho(p^k) \leq \sum_{i=1}^{\kappa} \varrho(H_i, p^k) \ll 1,$$

by (2.1). Hence it follows that

$$\varrho(p^k) = O_k(1), \quad (2.3)$$

for any prime  $p$  and any  $k \in \mathbb{N}$ .

## 3. THE DHR WEIGHTED SIEVE

We begin by recalling the set-up for a version of the DHR weighted sieve [5] that we shall use. Let  $\mathcal{A}$  be a finite sequence of integers. Under suitable hypotheses, the DHR weighted sieve produces a lower bound for the cardinality

$$\#\{a \in \mathcal{A} : \Omega(a) \leq r, (a, P(z)) = 1\},$$

for suitable  $r$  and  $z$ . In fact, in the literature, it is usually recorded as a lower bound for  $\#\{a \in \mathcal{A} : \Omega(a) \leq r\}$ , but the results are actually valid for the restricted cardinality in which

any  $a \in \mathcal{A}$  is forbidden to have prime factors less than  $z$ . (See the proof of [6, Thm. 11.1] for elucidation of this point.) In order to get a lower bound for  $\Sigma_1$  we take

$$\mathcal{A} = \{H(n) : n \leq x\}$$

and  $z = x^{1/v}$ , for a parameter  $v > 1$ .

When  $\kappa = 1$ , one can solve the differential-delay problem explicitly, and this leads to the conclusion that  $r = h + 1$  is admissible for every  $h \geq 1$  (see [20]). Moreover, for  $\kappa = 1$  and  $h \leq 2$  we may take  $r = h$  by the prime number theorem for arithmetic progressions and [18]. These values are reflected in Table 1.

For  $\kappa \geq 2$  we refer to [5]. One sees that we have a sieve of dimension  $\kappa$ , that all of the hypotheses of [5, Thm 1] are met with  $X = x$ ,  $\omega(d) = \varrho(d)$ ,  $\tau = 1$  and that the choice  $\mu = h$  is acceptable. For any  $v, w \in \mathbb{R}_{>0}$  satisfying  $v > w + 1$ , it therefore follows that

$$\#\{n \leq x : \Omega(H(n)) \leq r, (H(n), P(x^{1/v})) = 1\} \gg \frac{x}{(\log x)^\kappa},$$

provided that  $r \geq \lfloor R(v, w) \rfloor$ , where

$$R(v, w) = \frac{hv}{v-w} + \frac{\kappa}{f(v)} \int_w^{v-1} F(u) ((v-u)^{-1} - (v-w)^{-1}) du \quad (3.1)$$

and  $f, F$  is a pair of solutions to the following differential-delay problem:

**Theorem 3.1** (Diamond, Halberstam and Richert [8, 9, 10]). *Let  $\kappa > 1$  be a real number, and let  $\sigma : \mathbb{R}_{>0} \rightarrow \mathbb{R}$  be the continuous solution of the system*

$$\begin{aligned} u^{-\kappa} \sigma(u) &= \frac{(2e^\gamma)^{-\kappa}}{\Gamma(1+\kappa)} && \text{for } u \in (0, 2], \\ \frac{d}{du}(u^{-\kappa} \sigma(u)) &= -\kappa u^{-\kappa-1} \sigma(u-2) && \text{for } u > 2. \end{aligned} \quad (3.2)$$

*Then there are real numbers  $\alpha > \beta > 2$  such that the system*

$$\begin{aligned} F(u) &= \frac{1}{\sigma(u)} && \text{for } u \in (0, \alpha], \\ f(u) &= 0 && \text{for } u \in (0, \beta], \\ \frac{d}{du}(u^\kappa F(u)) &= \kappa u^{\kappa-1} f(u-1) && \text{for } u > \alpha, \\ \frac{d}{du}(u^\kappa f(u)) &= \kappa u^{\kappa-1} F(u-1) && \text{for } u > \beta \end{aligned} \quad (3.3)$$

*has continuous solutions  $F, f : \mathbb{R}_{>0} \rightarrow \mathbb{R}$  such that  $F(u)$  decreases monotonically,  $f(u)$  increases monotonically, and*

$$F(u) = 1 + O(e^{-u}), \quad f(u) = 1 + O(e^{-u}).$$

Now it is clear that

$$\Sigma_1 \geq \#\{n \leq x : \Omega(H(n)) \leq r, (H(n), P(x^{1/v})) = 1\}$$

if  $\delta < 1/v$ . We therefore conclude that  $\Sigma_1 \gg x/(\log x)^\kappa$  provided that  $r \geq \lfloor R(v, w) \rfloor$  and  $\delta < 1/v$ , which is plainly satisfactory for Theorem 1.1.

#### 4. LARGE SQUARE DIVISORS

The goal of this section is to prove the upper bound (1.1) for  $\Sigma_2$ . Our treatment is modelled on an argument of Hooley [16, Chapter 4]. We partition the interval  $(x^\delta, \infty)$  into  $I_1 \cup I_2 \cup I_3$ , where

$$I_1 = (x^\delta, x^{1-\delta}], \quad I_2 = (x^{1-\delta}, x^{1+\delta}], \quad I_3 = (x^{1+\delta}, \infty).$$

We clearly have

$$\Sigma_2 \leq \Sigma_{2,1} + \Sigma_{2,2} + \Sigma_{2,3},$$

where  $\Sigma_{2,i}$  is the number of  $n \leq x$  such that  $p^2 \mid H(n)$  for some prime  $p \in I_i$ .

We now make the further assumption that  $\delta < 1/11$ . Once taken together, the following three results suffice to establish (1.1), as required to complete the proof of Theorem 1.1.

**Lemma 4.1.** *We have  $\Sigma_{2,1} = O(x^{1-\delta})$ .*

*Proof.* Breaking the sum into residue classes modulo  $p^2$ , we find that

$$\Sigma_{2,1} \leq \sum_{p \in I_1} \sum_{\substack{\nu \bmod p^2 \\ H(\nu) \equiv 0 \bmod p^2}} \#\{n \leq x : n \equiv \nu \bmod p^2\}.$$

The inner cardinality is  $x/p^2 + O(1)$ . Hence

$$\Sigma_{2,1} \ll \sum_{p \in I_1} \left( \frac{x}{p^2} + 1 \right) \ll x^{1-\delta},$$

since  $\varrho(p^2) = O(1)$  by (2.3). This establishes the result.  $\square$

**Lemma 4.2.** *We have  $\Sigma_{2,3} = O(x^{1-\delta+\varepsilon})$ , for any  $\varepsilon > 0$ .*

*Proof.* The contribution to  $\Sigma_{2,3}$  from  $n \leq x$  such that  $H(n) = 0$  is  $O(1)$ , which is satisfactory. Hence we may focus on  $n$  for which  $H(n) \neq 0$ . We assume that  $x$  is large so that  $p \nmid \Delta$ , whenever  $p > x^{1+\delta}$ , where  $\Delta$  is given by (2.2). But then  $p^2 \mid H(n)$  implies that  $p^2 \mid H_i(n)$  for some  $i \in \{1, \dots, \kappa\}$ , since  $p$  doesn't divide any of the resultants  $\text{Res}(H_i, H_j)$ . In particular only the irreducible factors of degree 3 occur, since  $x^{d_i} \gg |H_i(n)| \geq p^2 \gg x^{2+2\delta}$ . It follows that

$$\begin{aligned} \Sigma_{2,3}(x) &\leq \sum_{\substack{1 \leq i \leq \kappa \\ d_i=3}} \#\{(n, p, m) : H_i(n) = p^2 m, n \leq x, p > x^{1+\delta}, m \ll x^{1-2\delta}\} \\ &\leq \sum_{\substack{1 \leq i \leq \kappa \\ d_i=3}} \sum_{m \ll x^{1-2\delta}} \#\{n \leq x : H_i(n) \equiv 0 \bmod m, H_i(n)/m = \square\}. \end{aligned}$$

Breaking into residue classes modulo  $m$  the inner cardinality is seen to be

$$\sum_{\substack{\nu \bmod m \\ H_i(\nu) \equiv 0 \bmod m}} \#\{n \leq x : n \equiv \nu \bmod m, H_i(n)/m = \square\}.$$

We make the change of variables  $n = \nu + mu$  for  $|u| \leq x/m + 1$ .

At this point we call upon work of Heath-Brown [14, Thm. 15] to estimate the inner cardinality. Given  $\varepsilon > 0$  and an absolutely irreducible polynomial  $F \in \mathbb{Z}[u, v]$  of degree  $d$ , this shows that there are at most

$$\ll (UV)^\varepsilon \exp\left(\frac{\log U \log V}{\log T}\right)$$

choices of  $(u, v) \in \mathbb{Z}^2$  such that  $|u| \leq U$ ,  $|v| \leq V$  and  $F(u, v) = 0$ . Here  $T$  is defined to be the maximum of  $U^{e_1}V^{e_2}$ , taken over all monomials  $u^{e_1}v^{e_2}$  which appear in  $F(u, v)$  with non-zero coefficient. Moreover, the implied constant is only allowed to depend on  $d$  and  $\varepsilon$ . We shall apply this bound with  $U = x/m + 1$  and  $F(u, v) = H_i(\nu + mu) - mv^2$ . In particular we may take  $T \geq V^2$ . Thus it follows that

$$\Sigma_{2,3}(x) \ll \sum_{\substack{1 \leq i \leq \kappa \\ d_i=3}} \sum_{m \leq x^{1-2\delta}} \varrho(H_i, m) \left(\frac{x}{m}\right)^{1/2+\varepsilon},$$

for any  $\varepsilon > 0$ . We now factorise  $m = st$  where  $s$  is cube-free and  $t$  is cube-full, with  $(s, t) = 1$ . Then

$$\Sigma_{2,3}(x) \ll x^{1/2+\varepsilon} \sum_{\substack{1 \leq i \leq \kappa \\ d_i=3}} \sum_{\substack{t \leq x^{1-2\delta} \\ t \text{ cube-full}}} \frac{\varrho(H_i, t)}{\sqrt{t}} \sum_{\substack{s \leq x^{1-2\delta}/t \\ s \text{ cube-free}}} \frac{\varrho(H_i, s)}{\sqrt{s}}.$$

Now it follows from (2.1) that  $\varrho(H_i, s) \ll s^\varepsilon$  and  $\varrho(H_i, t) \ll t^{2/3+\varepsilon}$ . Hence

$$\Sigma_{2,3}(x) \ll x^{1/2+\varepsilon} \sum_{\substack{t \leq x^{1-2\delta} \\ t \text{ cube-full}}} \frac{t^{2/3+\varepsilon}}{\sqrt{t}} \left(\frac{x^{1-2\delta}}{t}\right)^{1/2+\varepsilon} \ll x^{1-\delta+3\varepsilon},$$

since

$$\sum_{\substack{t \leq T \\ t \text{ cube-full}}} \frac{1}{t^{1/3}} \ll T^\varepsilon.$$

We complete the proof of the lemma on redefining the choice of  $\varepsilon$ . □

**Lemma 4.3.** *We have  $\Sigma_{2,2} = O(x^{10/11+\delta})$ .*

*Proof.* As previously, if  $x$  is large enough we have  $p \nmid \Delta$  whenever  $p \in I_2$ . Thus

$$\Sigma_{2,2}(x) \leq \sum_{1 \leq i \leq \kappa} \# \{n \leq x : \exists p \in I_2 \text{ s.t. } p^2 \mid H_i(n)\} = \sum_{1 \leq i \leq \kappa} \Sigma_{2,2}^{(i)},$$

say. Suppose first that  $i \in \{1, \dots, \kappa\}$  is such that  $d_i = \deg(H_i) \leq 2$ . Then we can assume that  $H_i(n) = p^2 m$  with  $m \leq x^2/x^{2(1-\delta)} = x^{2\delta}$ . Arguing as in the proof of the previous lemma we find that

$$\Sigma_{2,2}^{(i)} \ll \sum_{m \leq x^{2\delta}} \varrho(H_i, m) \left(\frac{x}{m}\right)^{1/2+\varepsilon}.$$

Breaking  $m$  into its cube-free and cube-full part, we are easily led to the satisfactory contribution  $\Sigma_{2,2}^{(i)} = O(x^{1/2+\delta+2\varepsilon})$ .

Now suppose that  $i \in \{1, \dots, \kappa\}$  is such that  $d_i = 3$ . To estimate  $\Sigma_{2,2}^{(i)}$  we shall call upon work of Reuss [19]. Thus we have the overall contribution

$$\Sigma_{2,2}^{(i)} \ll x^\varepsilon \max_{X \ll x} \max_{\substack{X^{1-\delta} \ll A \ll X^{1+\delta} \\ X^{1-2\delta} \ll B \ll X^{1+2\delta}}} \mathcal{N}(X; A, B),$$

where

$$\mathcal{N}(X; A, B) = \#\{(n, a, b) : n \sim X, a \sim A, b \sim B, \mu^2(a) = 1, H_i(n) = a^2 b\}$$

in the notation of [19, Lemma 3]. Appealing to [19, page 283] with  $d = 3$  one finds that  $\mathcal{N}(X; A, B) \ll M^{2/3} X^{2/3+\varepsilon}$ , where  $M$  is any choice of parameter satisfying the condition

$$(AB)^{3/11} X^{-2/11} \ll M \ll \min\{X^{1/2}, A^{1/2}\}$$

from [19, Lemma 7]. A moment's thought shows that  $M = X^{4/11+\delta}$  is admissible, which leads to the bound  $\mathcal{N}(X; A, B) \ll X^{10/11+2\delta/3+\varepsilon}$ . We conclude the proof of the lemma by inserting this into our bound for  $\Sigma_{2,2}^{(i)}$  and taking  $\varepsilon$  sufficiently small in terms of  $\delta$ .  $\square$

## 5. NUMERICAL ESTIMATES

In this section, we describe how to compute rigorous numerical approximations of (3.1). Since our main application requires only integer values of  $\kappa \geq 2$ , we make this restriction for convenience. However, our approach should work just as well for arbitrary real  $\kappa \geq 1$ , and in fact one could likely treat  $\kappa$  as a variable. This might be useful, for instance, for extending the results of [7] to small  $\kappa$ . (On the other hand, recent work of Franze [12] and Blight [1] has shown that lower-bound sieves that are superior to the DHR sieve are possible once  $\kappa \geq 3$ , so such an extension is likely to be of limited interest.)

**5.1. Generalised polynomial representations of continuous functions.** We begin with some generalities on representing continuous functions by (generalised) polynomials before getting into the details of computing (3.1) below.

Let  $f : [0, 1] \rightarrow \mathbb{R}$  be a continuous function. For a fixed  $N \in \mathbb{Z}_{\geq 0}$ , we consider representations of  $f$  of the form

$$f(z) = \sum_{n=0}^N f_n(z) z^n, \tag{5.1}$$

where each  $f_n$  is a bounded function on  $[0, 1]$ . For instance, if  $f$  is smooth then there is such a representation with  $f_n = \frac{f^{(n)}(0)}{n!}$  for  $n < N$  and  $f_N$  smooth. We represent each coefficient  $f_n$  by an interval with rational endpoints containing the image  $f_n([0, 1])$ .

Given an interval  $[a, b]$ , let  $\Theta([a, b])$  denote any function (possibly different at each occurrence) whose image lies in  $[a, b]$ . The algebraic and analytic operations on series of the form (5.1) are implemented in a straightforward manner. We mention a few in particular:

- If  $f(z) = \sum_{n=0}^N f_n(z) z^n$  and  $g(z) = \sum_{n=0}^N g_n(z) z^n$  then

$$f(z)g(z) = \sum_{n=0}^N h_n(z) z^n,$$

8



where  $h_n(z) = \sum_{i+j=n} f_i(z)g_j(z)$  for  $n < N$  and

$$h_N(z) = \sum_{i+j \geq N} f_i(z)g_j(z)z^{i+j-N}.$$

We obtain a bounding interval for  $h_N$  by evaluating the above in interval arithmetic with  $z$  replaced by  $\Theta([0, 1])$ .

- If  $f$  is known to be bounded away from 0 then we may compute a representation for its reciprocal via

$$\frac{1}{f(z)} = \sum_{n=0}^N k_n(z)z^n, \quad (5.2)$$

where  $k_n$  is defined for  $n < N$  by the relation

$$\sum_{n=0}^{N-1} f_n z^n \cdot \sum_{n=0}^{N-1} k_n z^n \equiv 1 \pmod{z^N},$$

and

$$k_N(z) = -\frac{1}{f(z)} \sum_{\substack{i \leq N, j < N \\ i+j \geq N}} f_i(z)k_j(z)z^{i+j-N}.$$

To compute a bounding interval for  $k_N$  we again use interval arithmetic, replacing  $f(z)$  in the denominator by a known bounding interval.

- We have

$$\exp f(z) = e^{f_0(z)} \prod_{n=1}^N \left( \sum_{j=0}^{\lceil N/n \rceil - 1} \frac{f_n(z)^j}{j!} z^{nj} + R_{n,N}(z)z^N \right),$$

where

$$R_{n,N}(z) = \sum_{j=\lceil N/n \rceil}^{\infty} \frac{f_n(z)^j z^{nj-N}}{j!}.$$

Using the Lagrange form of the remainder term in Taylor's theorem, we have

$$\begin{aligned} R_{n,N}(z) &= \frac{f_n(z)^{\lceil N/n \rceil}}{\lceil N/n \rceil!} \exp(\Theta([0, 1])f_n(z)z^n) z^{n\lceil N/n \rceil - N} \\ &= \Theta([0, 1]) \frac{f_n(z)^{\lceil N/n \rceil}}{\lceil N/n \rceil!} \exp(\Theta([0, 1])f_n(z)). \end{aligned}$$

Given a bounding interval for  $f_n$ , this yields one for  $R_{n,N}$  via interval arithmetic.

- Let  $I_n$  be a bounding interval for  $f_n$ . Then we have

$$\begin{aligned} \int_0^z f(x) dx &= \sum_{n=0}^N \int_0^z f_n(x)x^n dx = \sum_{n=0}^N \frac{\Theta(I_n)}{n+1} z^{n+1} \\ &= \sum_{n=1}^N \frac{\Theta(I_{n-1})}{n} z^n + \Theta([0, 1]) \frac{\Theta(I_N)}{N+1} z^N. \end{aligned}$$

We conclude with two useful examples employing the Lagrange form of the remainder term. First, if  $\nu \in \mathbb{R}_{>0}$  then

$$(1+x)^{-\nu} = \sum_{n=0}^{N-1} (-1)^n \binom{n+\nu-1}{n} x^n + (-1)^N \binom{N+\nu-1}{N} \Theta([0,1]) x^N \quad \text{for } x \in \mathbb{R}_{\geq 0}.$$

Similarly,

$$e^x = \sum_{n=0}^{N-1} \frac{x^n}{n!} + \frac{e^{\Theta([0,1])x} x^N}{N!} \quad \text{for } x \in \mathbb{R}.$$

**5.2. Solving the differential-delay system.** Next we describe how to compute the solution to Theorem 3.1 for integral  $\kappa \geq 2$ , beginning with  $\alpha$  and  $\beta$ . These are found via a number of auxiliary functions. First, we have  $p, q : \mathbb{R}_{>0} \rightarrow \mathbb{R}$  defined by the differential-delay equations

$$\frac{d}{du}(up(u)) = \kappa(p(u) - p(u+1)), \quad \lim_{u \rightarrow \infty} up(u) = 1$$

and

$$\frac{d}{du}(uq(u)) = \kappa(q(u) + q(u+1)), \quad \lim_{u \rightarrow \infty} u^{1-2\kappa} q(u) = 1. \quad (5.3)$$

Second,  $\tilde{\Pi}, \tilde{\Xi} : (2, \infty) \rightarrow \mathbb{R}$  are defined by

$$\begin{aligned} \tilde{\Pi}(u) &= \frac{up(u)}{\sigma(u)} + \kappa \int_{u-2}^u \frac{p(t+1)}{\sigma(t)} dt, \\ \tilde{\Xi}(u) &= \frac{uq(u)}{\sigma(u)} - \kappa \int_{u-2}^u \frac{q(t+1)}{\sigma(t)} dt. \end{aligned} \quad (5.4)$$

Then for  $\alpha, \beta$  we may take any solution to the pair of equations

$$\begin{aligned} \tilde{\Pi}(\alpha) + \kappa(\alpha-1)^{1-\kappa} p(\alpha-1) \int_{\beta}^{\alpha-1} \frac{t^{\kappa-1}}{\sigma(t-1)} dt &= 2, \\ \tilde{\Xi}(\alpha) - \kappa(\alpha-1)^{1-\kappa} q(\alpha-1) \int_{\beta}^{\alpha-1} \frac{t^{\kappa-1}}{\sigma(t-1)} dt &= 0. \end{aligned} \quad (5.5)$$

(Conjecturally, the solution is unique.) We describe the computation of each piece in turn.

**5.2.1. Computing  $p$ .** By [6, (12.11)], we have the following integral representation for  $p$ :

$$p(u) = \int_0^{\infty} \exp(-\kappa \operatorname{Ein}(x) - ux) dx, \quad (5.6)$$

where

$$\operatorname{Ein}(x) = \int_0^x \frac{1-e^{-t}}{t} dt = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n \cdot n!} x^n. \quad (5.7)$$

We split the integral (5.6) as

$$\begin{aligned} & \sum_{m=0}^{M-1} \int_m^{m+1} \exp(-\kappa \operatorname{Ein}(x) - ux) dx + \int_M^{\infty} \exp(-\kappa \operatorname{Ein}(x) - ux) dx \\ &= \sum_{m=0}^{M-1} e^{-mu} \int_0^1 \exp(-\kappa \operatorname{Ein}(m+z) - uz) dz + \int_M^{\infty} \exp(-\kappa \operatorname{Ein}(x) - ux) dx \end{aligned}$$

for some  $M \in \mathbb{Z}_{>0}$ . For the final term, we use the crude estimate  $\text{Ein}(x) \geq \text{Ein}(M)$ , so that

$$\int_M^\infty \exp(-\kappa \text{Ein}(x) - ux) dx = \Theta([0, 1]) u^{-1} e^{-\kappa \text{Ein}(M) - Mu}.$$

Using the series in (5.7), for any positive integer  $N$  and any  $z \in [0, 1]$ , we have

$$\text{Ein}(z) = \sum_{n=1}^{N-1} \frac{(-1)^{n-1}}{n \cdot n!} z^n + \Theta([0, 1]) \frac{(-1)^{N-1}}{N \cdot N!} z^N. \quad (5.8)$$

On the other hand, differentiating the integral representation in (5.7), we have

$$\text{Ein}^{(k)}(x) = (-1)^{k-1} (k-1)! x^{-k} \left( 1 - e^{-x} \sum_{n=0}^{k-1} \frac{x^n}{n!} \right), \quad (5.9)$$

so that

$$0 \leq (-1)^{k-1} \frac{\text{Ein}^{(k)}(x)}{k!} = \frac{1}{k} e^{-x} \sum_{n=0}^{\infty} \frac{x^n}{(n+k)!} \leq \frac{1}{k \cdot k!}.$$

Comparing series term by term, we see that for any fixed  $x > 0$ , the sequence  $\text{Ein}^{(k)}(x)/k!$  is alternating and decreasing in magnitude. Hence,

$$\text{Ein}(m+z) = \sum_{n=0}^{N-1} \frac{\text{Ein}^{(n)}(m)}{n!} z^n + \Theta([0, 1]) \frac{\text{Ein}^{(N)}(m)}{N!} z^N \quad \text{for } z \in [0, 1].$$

For each  $m \in \{0, 1, \dots, M-1\}$ , we use (5.8) and (5.9) to compute an expansion for  $\text{Ein}(m+z)$  for  $z \in [0, 1]$ . (The constant terms  $\text{Ein}(m)$  are computed recursively using the expansion for  $m-1$ .) Applying the algorithms from §5.1, we obtain an expansion of the form

$$\exp(-\kappa \text{Ein}(m+z)) = \sum_{n=0}^N a_{m,n}(z) z^n \quad \text{for } z \in [0, 1].$$

Thus,

$$p(u) = \sum_{m=0}^{M-1} e^{-mu} \sum_{n=0}^N \int_0^1 a_{m,n}(z) z^n e^{-uz} dz + \Theta([0, 1]) u^{-1} e^{-\kappa \text{Ein}(M) - Mu}.$$

Now fix  $u_0 \geq 2$  and replace  $u$  in the above by  $u_0 + u$  for some  $u \in [0, 1]$ . Then

$$e^{-(u_0+u)z} = e^{-u_0 z} \sum_{r=0}^N b_r(z, u) z^r u^r,$$

where

$$b_r(z, u) = \begin{cases} \frac{(-1)^r}{r!} & \text{if } r < N, \\ \Theta([0, 1]) \frac{(-1)^N}{N!} & \text{if } r = N. \end{cases}$$

Thus,

$$\begin{aligned}
p(u_0 + u) &= \sum_{m=0}^{M-1} \sum_{r=0}^N c_{u_0, m, r}(u) e^{-mu} u^r + \Theta([0, 1]) u_0^{-1} e^{-\kappa \text{Ein}(M) - Mu_0} \\
&= \sum_{r=0}^N \sum_{m=0}^{M-1} c_{u_0, m, r}(u) \left( \sum_{n=0}^{N-r-1} \frac{(-m)^n}{n!} u^{n+r} + \Theta([0, 1]) \frac{(-m)^{N-r}}{(N-r)!} u^N \right) \\
&\quad + \Theta([0, 1]) u_0^{-1} e^{-\kappa \text{Ein}(M) - Mu_0},
\end{aligned} \tag{5.10}$$

where

$$\begin{aligned}
c_{u_0, m, r}(u) &= e^{-mu_0} \sum_{n=0}^N \int_0^1 a_{m, n}(z) b_r(z, u) z^{n+r} e^{-u_0 z} dz \\
&= e^{-mu_0} \sum_{n=0}^N \Theta(I_{m, n, r}) \int_0^1 z^{n+r} e^{-u_0 z} dz,
\end{aligned}$$

and  $I_{m, n, r}$  is a bounding interval for  $a_{m, n} b_r$ . To compute the integral on the last line accurately, we rely on **Arb**'s routines for the confluent hypergeometric function  $M$ , via the identity

$$\int_0^1 z^n e^{-u_0 z} dz = \frac{1}{n+1} M(n+1, n+2, -u_0).$$

This yields an expansion of the form

$$p(u_0 + u) = \sum_{n=0}^N p_{u_0, n}(u) u^n \quad \text{for } u \in [0, 1].$$

For small  $u_0$ , the worst case error in (5.10) occurs when  $m \approx N/u_0$ , and is roughly of size  $u_0^{-N}$ . If we aim for  $B$  bits of precision for all  $u_0 \geq 2$ , then a sensible choice of parameters is  $N = B$ ,  $M = \lceil \frac{B \log 2}{u_0} \rceil$ .

**5.2.2. Computing  $q$ .** Since we have restricted to positive integer values of  $\kappa$ , it turns out that  $q$  is a polynomial of degree  $2\kappa - 1$ . If we put  $q(u) = \sum_{n=0}^{2\kappa-1} a_n u^n$  then, solving (5.3), we find that the coefficients  $a_n$  are given recursively by

$$a_{2\kappa-1} = 1, \quad a_r = -\frac{\kappa}{2\kappa-1-r} \sum_{n=r+1}^{2\kappa-1} \binom{n}{r} a_n \quad \text{for } r < 2\kappa-1.$$

Once the  $a_n$  have been computed, we work out the coefficients of  $q(u_0 + u)$  for integers  $u_0 \geq 1$  by polynomial arithmetic. In order to limit the precision loss, we perform these computations in rational arithmetic first before converting to floating point intervals.

**5.2.3. Computing  $\sigma$ .** Let  $u_0 \in \mathbb{Z}_{\geq 0}$ . We wish to compute an expansion of the form

$$\sigma(u_0 + u) = \sum_{n=0}^N \sigma_{u_0, n}(u) u^n \quad \text{for } u \in [0, 1].$$

For  $u_0 = 0$  we have

$$\sigma(u) = A^{-1} u^\kappa \quad \text{for } u \in [0, 1],$$

where  $A = \kappa!(2e^\gamma)^\kappa$ , which is an expansion of the above type provided that  $N \geq \kappa$ . For  $u_0 = 1$  we similarly have

$$\sigma(1+u) = A^{-1}(1+u)^\kappa = A^{-1} \sum_{n=0}^{\kappa} \binom{\kappa}{n} u^n \quad \text{for } u \in [0, 1].$$

Next, suppose that an expansion of the desired type is known for  $u_0 - 2$  and  $u_0 - 1$ . Solving (3.2), we have

$$\sigma(u_0 + u) = \left(1 + \frac{u}{u_0}\right)^\kappa \left[ \sigma(u_0) - \frac{\kappa}{u_0} \int_0^u \left(1 + \frac{t}{u_0}\right)^{-\kappa-1} \sigma(u_0 - 2 + t) dt \right].$$

Using the expansion around  $u_0 - 1$  to estimate  $\sigma(u_0)$  and applying the formulas and algorithms from §5.1 in a straightforward way, we obtain an expansion for  $\sigma(u_0 + u)$ .

**5.2.4. Computing  $1/\sigma$ .** For  $u_0 \geq 3$ , we use (5.2), together with the fact that  $\sigma$  is monotonic [6, (14.6)] to obtain a bounding interval, to compute an expansion for  $1/\sigma(u_0 + u)$ . For  $u_0 \in \{1, 2\}$ , this method gives a poor approximation when  $u$  is close to 1 since, in each case, the analytic function that agrees with  $\sigma(u_0 + u)$  on  $[0, 1]$  has a zero at or just to the left of  $u = -1$ . This can be mitigated in various ways, e.g. by using expansions around  $u_0 = 3/2$  or  $5/2$  instead. In order to keep our later algorithms as simple and uniform as possible, we use the following *ad hoc* methods to obtain better polynomial approximations of  $1/\sigma(u_0 + u)$  for  $u_0 \in \{1, 2\}$ .

First, for  $u_0 = 1$  and  $u \in [0, 1]$ , we have

$$(1+u)^{-\kappa} = 2^{-\kappa} \left(1 - \frac{1-u}{2}\right)^{-\kappa} = \sum_{n=0}^{\infty} 2^{-\kappa-n} \binom{\kappa+n-1}{n} (1-u)^n.$$

We truncate the series at  $N$  and express it in the form  $\sum_{n=0}^N c_n u^n$  by polynomial arithmetic. Since the series has positive terms, the greatest error occurs at  $u = 0$ . Hence, to account for the error, it suffices to replace the constant term  $c_0$  by  $\Theta([c_0, 1])$ .

Turning to  $u_0 = 2$ , we solve (3.2) to find, for  $u \in [0, 1]$ ,

$$\begin{aligned} A\sigma(3-u) &= (3-u)^\kappa \left(1 - \kappa \log\left(\frac{3-u}{2}\right)\right) + \kappa \sum_{n=1}^{\kappa} \frac{(1-u)^n (3-u)^{\kappa-n}}{n} \\ &= (3-u)^\kappa \left(1 - \kappa \log \frac{3}{2} + \kappa \sum_{n=1}^{\infty} \frac{u^n}{n 3^n}\right) + \kappa \sum_{n=1}^{\kappa} \frac{(1-u)^n (3-u)^{\kappa-n}}{n} \\ &= (3-u)^\kappa \left(1 - \kappa \log \frac{3}{2} + \kappa \sum_{n=1}^N \frac{u^n}{n 3^n} + \frac{\kappa \Theta([0, 1])}{2(N+1)3^N} u^{N+1}\right) \\ &\quad + \kappa \sum_{n=1}^{\kappa} \frac{(1-u)^n (3-u)^{\kappa-n}}{n}. \end{aligned} \tag{5.11}$$

We compute this series using the arithmetic of §5.1 and invert it to obtain a degree- $(N+1)$  approximation for  $1/\sigma(3-u)$ . Since the error in (5.11) is concentrated in the highest-degree term, the same is true of our approximation to the inverse. Hence, in the degree- $N$  polynomial part we may replace  $u$  by  $1-u$  without excessive precision loss. (There is some loss due to cancellation between terms, but that can be compensated for by increasing the

working precision.) In the final term, we simply replace  $u^{N+1}$  by  $\Theta([0, 1])$  and incorporate it into the constant term.

Finally, for  $u_0 = 0$ ,  $1/\sigma(u_0 + u) = Au^{-\kappa}$  has an unavoidable singularity at  $u = 0$ . However, the computation of  $1/\sigma$  in this region is only needed in order to compute the integrals  $\int_w^{v-1} F(u) du$  and  $\int_w^{v-1} \frac{F(u)}{v-u} du$ , and we can evaluate the contribution from  $u \in [w, 1]$  by elementary means, as detailed below.

**5.2.5. Computing  $\tilde{\Pi}$  and  $\tilde{\Xi}$ .** For integers  $u_0 \geq 2$ , we compute expansions for  $\tilde{\Pi}(u_0 + u)$  and  $\tilde{\Xi}(u_0 + u)$  via (5.4), using our expansions for  $p$ ,  $q$ ,  $1/\sigma$  and a straightforward application of the operations from §5.1.

**5.2.6. Computing  $\alpha$  and  $\beta$ .** With these preliminaries in place, we can now proceed with the computation of  $\alpha$  and  $\beta$ . First, eliminating the integral terms in (5.5), we see that  $\alpha$  is a root of the function

$$l(u) = (\tilde{\Pi}(u) - 2)q(u - 1) + \tilde{\Xi}(u)p(u - 1).$$

In [7] it was shown that  $l$  has a root satisfying  $\varrho + 1 < \alpha < \varrho + O(1)$ , where  $\varrho$  denotes the greatest real zero of  $q$ . In every case that we examined we found that  $l(\varrho + 1)l(\varrho + 2) < 0$ , so there is a solution  $\alpha \in (\varrho + 1, \varrho + 2)$ . (In [6, Prop. 17.3] it is proven that there is a solution with  $\alpha < 3.75\kappa$ , so it is not necessary to assume that  $\alpha < \varrho + 2$ , but we did so for efficiency.) To locate it precisely, we compute expansions for  $l(u_0 + u)$  as above and apply bisection<sup>1</sup>, beginning with the interval  $(\varrho + 1, \varrho + 2)$ .

Once  $\alpha$  has been found,  $\beta < \alpha - 1$  is uniquely determined by (5.5), since  $\frac{t^{\kappa-1}}{\sigma(t-1)} > 0$  and  $\frac{\tilde{\Xi}(\alpha)}{q(\alpha-1)} > 0$  [6, (17.9)]. By [9, Prop. 7.3] and [6, Table 17.1], we have  $\beta > 2\kappa$  for all integral  $\kappa \geq 2$ ; to locate it we compute expansions for  $\kappa \int_{u_0+u}^{\alpha-1} \frac{t^{\kappa-1}}{\sigma(t-1)} dt$  and again apply bisection, beginning with the interval  $(2\kappa, \alpha - 1)$ .

Our computed values of  $\alpha$  and  $\beta$  for  $\kappa \leq 50$  are displayed to 20 decimal place accuracy at [3].

**5.2.7. Computing  $F$  and  $f$ .** We compute expansions for  $F(u_0 + u)$  and  $f(u_0 + u)$  by a similar strategy to that for  $\sigma$ . Note that for  $u_0 \geq \lfloor \alpha \rfloor$ ,  $F(u_0 + u)$  changes behaviour at  $u = \{\alpha\} = \alpha - \lfloor \alpha \rfloor$ , and similarly for  $f(u_0 + u)$  when  $u_0 \geq \lfloor \alpha \rfloor + 1$ . Hence, for each  $u_0$ , we compute two approximations for  $F(u_0 + u)$  and  $f(u_0 + u)$ , one valid for  $u \in [0, \{\alpha\}]$  and one for  $u \in [\{\alpha\}, 1]$ . Solving (3.3), we have

$$F(u_0 + u) = \left(1 + \frac{u}{u_0}\right)^{-\kappa} \left[ c + \frac{\kappa}{u_0} \int_0^u \left(1 + \frac{t}{u_0}\right)^{\kappa-1} f(u_0 - 1 + t) dt \right],$$

where  $c$  is chosen to ensure continuity at  $u = 0$  or  $u = \{\alpha\}$ , and similarly with the roles of  $F$  and  $f$  reversed. Applying this iteratively yields the desired expansions.

---

<sup>1</sup>Since we store all numbers as intervals, if it happens that  $\alpha$  is very close to an integer then it might not be possible to decide which value of  $u_0$  to use at some point during the bisection algorithm. One could handle this by taking the union of the intervals arising from all relevant values of  $u_0$ . However, we expect that this does not occur generically; in our implementation, we simply output an error message and exit when it occurs, and we never observed it in practice. The same issue arises at various points for computing  $\beta$ , as well as the parameters  $v$  and  $w$  below. We handled these in a similar fashion and proceed without further comment.

5.3. **Optimising**  $R(v, w)$ . Differentiating (3.1), we find that

$$f(v)(v-w)^2 \frac{\partial R}{\partial w} = hvf(v) - \kappa \int_w^{v-1} F(u) du. \quad (5.12)$$

Further, we have

$$\begin{aligned} \frac{d}{dv} \left( hvf(v) - \kappa \int_{\beta-1}^{v-1} F(u) du \right) &= h(f(v) + vf'(v)) - \kappa F(v-1) \\ &= (h - \kappa)F(v-1) + h(1 - \kappa^{-1})vf'(v) > 0 \quad \text{for } v > \beta, \end{aligned}$$

and since  $[hvf(v) - \kappa \int_{\beta-1}^{v-1} F(u) du]_{v=\beta} = 0$ , it follows that  $hvf(v) - \kappa \int_{\beta-1}^{v-1} F(u) du > 0$  for all  $v > \beta$ .

Since  $F(u) > 1$  for all  $u$ , (5.12) is a strictly increasing function of  $w > 0$ . It tends to  $-\infty$  as  $w \rightarrow 0^+$  and, by the above, is positive at  $w = \beta - 1$ ; hence, for each fixed  $v > \beta$ , there is a unique  $w = w(v) \in (0, \beta - 1)$  at which  $R(v, w)$  is minimal. Given a value of  $v$ , we compute  $w(v)$  as follows. First we compute  $c(v) = hvf(v) - \kappa \int_2^{v-1} F(u) du$ . If  $c(v) \geq 0$  then  $w(v) \leq 2$ , and we have

$$c(v) = \kappa \int_{w(v)}^2 F(u) du = A\kappa \int_{w(v)}^2 u^{-\kappa} du = \frac{A\kappa}{\kappa - 1} (w(v)^{1-\kappa} - 2^{1-\kappa}),$$

which we then solve for  $w(v)$ . Otherwise,  $w(v) \in (2, \beta - 1)$ , and we find the root of (5.12) by bisection.

Replacing  $w$  by  $w(v)$  in (3.1) and applying (5.12), we have

$$R(v, w(v)) = \frac{\kappa}{f(v)} \int_{w(v)}^{v-1} \frac{F(u)}{v-u} du.$$

To compute the integral, we split it over the intervals  $[u_0, u_0 + \{\alpha\}]$  and  $[u_0 + \{\alpha\}, u_0 + 1]$  for each relevant integer  $u_0$ , taking the appropriate subinterval around the endpoints  $w(v)$  and  $v - 1$ . For each interval  $[u_1, u_2] \subseteq [u_0, u_0 + 1]$  with  $u_0 \geq 2$  we use the approximation

$$\frac{1}{v-u} = \frac{1}{(v-u_0) - (u-u_0)} = \sum_{n=0}^{N-1} (v-u_0)^{-n-1} (u-u_0)^n + \frac{(v-u_0)^{-N} (u-u_0)^N}{v - \Theta([u_1, u_2])}.$$

Note that we always have  $\frac{u_2-u_0}{v-u_0} \leq \frac{1}{2}$ , so this is accurate to at least  $N$  bits. When  $w(v) < 2$ , we compute the contribution from  $[w(v), 2]$  directly, via

$$\int_{w(v)}^2 \frac{du}{u^\kappa(v-u)} = \left[ v^{-\kappa} \log \frac{1}{v-u} - \sum_{n=1}^{\kappa-1} \frac{v^{n-\kappa} u^{-n}}{n} \right]_{u=w(v)}^{u=2}.$$

Thus, we have reduced the problem to one of minimising the single-variable function  $R(v) = R(v, w(v))$ . Presumably,  $R(v)$  has a unique local (and global) minimum on  $(\beta, \infty)$ ; although we are not aware of a proof of this, we found no violations of it in practice. Empirically, the optimal  $v$  is always larger than  $\alpha + 3$ . A good upper bound that is uniform in all parameters is not as easy to describe, but by trial and error we found that  $v < 200$  for every  $\kappa \leq h \leq 50$ . Hence, to compute the table in [3], we first worked out the expansions for  $F$  and  $f$  for all  $u_0 < 200$ . We then used a simple linear search through the points  $v = \lceil \alpha \rceil + n$  for  $n = 1, 2, 3 \dots$  to find one at which  $R(v) < \min(R(v-1), R(v+1))$ . Finally, we zoomed in on the minimum by a simple bisection algorithm.

**5.4. Working precision.** We conclude this section with a few words on numerical precision. Since our method for computing  $f$  and  $F$  is iterative, the total precision loss accumulates as  $u_0$  increases. This mainly affects large values of  $\kappa$ , for which the optimal  $v$  can be large. We counteracted this effect by increasing the working precision with  $\kappa$ . Empirically we found that using  $12(\kappa+10)$  bits of precision was enough to determine the minimum value of  $R(v, w)$  to at least 20 significant (decimal) digits, for all  $\kappa \leq h \leq 50$ . The demand for high precision is the main obstacle to extending our computations to larger values of  $\kappa$ , though we expect that  $\kappa$  in the hundreds would still be feasible.

## REFERENCES

- [1] S.E. Blight, *Refinements of Selberg's sieve*. Ph.D thesis, Rutgers University, 2010.
- [2] A.R. Booker and S.A. Irvine, The Euclid–Mullin graph. *J. Number Theory* **165** (2016), 30–57.
- [3] A.R. Booker and T.D. Browning, Extended table and source code for the algorithms presented here, <http://arxiv.org/src/1511.00601v2/anc/dhr.html>.
- [4] T.D. Browning and R. de la Bretèche, Sums of arithmetic functions over values of binary forms. *Acta Arith.* **125** (2006), 291–304.
- [5] H.G. Diamond and H. Halberstam, Some applications of sieves of dimension exceeding 1. *Sieve methods, exponential sums, and their applications in number theory (Cardiff, 1995)*, 101–107, London Math. Soc. Lecture Note Ser. **237**, Cambridge Univ. Press, Cambridge, 1997.
- [6] ———, *A higher-dimensional sieve method*, Cambridge Tracts in Math. **177**, Cambridge Univ. Press, Cambridge, 2008.
- [7] ———, On the sieve parameters  $\alpha_\kappa$  and  $\beta_\kappa$  for large  $\kappa$ . *J. Number Theory* **67** (1997), 52–84.
- [8] H.G. Diamond, H. Halberstam and H.-E. Richert, A boundary value problem for a pair of differential delay equations related to sieve theory. I. *Analytic number theory (Allerton Park, IL, 1989)*, 133–157, Progr. Math. **85**, Birkhäuser Boston, Boston, MA, 1990.
- [9] ———, A boundary value problem for a pair of differential delay equations related to sieve theory. II, *J. Number Theory* **45** (1993), 129–185.
- [10] ———, A boundary value problem for a pair of differential delay equations related to sieve theory. III. *J. Number Theory* **47** (1994), 300–328.
- [11] P. Erdős, Arithmetical properties of polynomials. *J. London Math. Soc.* **28** (1953), 416–425.
- [12] C. S. Franze, Sifting limits for the  $\Lambda^2\Lambda^-$  sieve. *J. Number Theory* **131** (2011), 1962–1982.
- [13] A. Granville,  $ABC$  allows us to count squarefrees. *Internat. Math. Res. Notices* **19** (1998), 991–1009.
- [14] D.R. Heath-Brown, Counting rational points on algebraic varieties. *Analytic number theory*, 51–95, Lecture Notes in Math. **1891**, Springer, Berlin, 2006.
- [15] C. Hooley, On the power free values of polynomials. *Mathematika* **14** (1967), 21–26.
- [16] C. Hooley, *Applications of sieve methods to the theory of numbers*. Cambridge Tracts in Math. **70**, Cambridge Univ. Press, Cambridge, 1976.
- [17] F. Johansson, Arb: a C library for ball arithmetic. *ACM Communications in Computer Algebra* **47** (2013), 166–169.
- [18] R.J. Lemke Oliver, Almost-primes represented by quadratic polynomials. *Acta Arith.* **151** (2012), 241–261.
- [19] T. Reuss, Power-free values of polynomials. *Bull. London Math. Soc.* **47** (2015), 270–284.
- [20] H.-E. Richert, Selberg's sieve with weights. *Mathematika* **16** (1969), 1–22.
- [21] F.S. Wheeler, *On two differential-difference equations arising in analytic number theory*. Ph.D. thesis, University of Illinois at Urbana-Champaign, 1988.

SCHOOL OF MATHEMATICS, UNIVERSITY OF BRISTOL, BRISTOL, BS8 1TW, UK  
*E-mail address:* `andrew.booker@bristol.ac.uk`

SCHOOL OF MATHEMATICS, UNIVERSITY OF BRISTOL, BRISTOL, BS8 1TW, UK  
*E-mail address:* `t.d.browning@bristol.ac.uk`